UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/637,229 | 08/11/2000 | Cetin K. Koc | 245-55512 | 7362 |

24197 7590 12/13/2005

KLARQUIST SPARKMAN, LLP
121 SW SALMON STREET
SUITE 1600
PORTLAND, OR 97204

| EXAMINER | |
|---|---|
| LAFORGIA, CHRISTIAN A | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/637,229 | KOC ET AL. | |
| | Examiner | Art Unit | |
| | Christian La Forgia | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1 and 3-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. The Amendment filed on 12 September 2005 has been noted and made of record.

2. Claims 1 and 3-21 have been presented for examination.

3. Claim 2 has been cancelled as per Applicant's request.

### *Response to Arguments*

4. Applicant's arguments filed 12 September 2005 have been fully considered but they are not persuasive.

5. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from specific areas of the references. The Applicant alleges that one of the multiplication circuits fails to disclose the limitation receiving a bit of the first parameter and partial words of the second, while admitting that the other multiplication circuit performs such functions. The Applicant fails to specifically point out any teaching, disclosure or suggestion in the cited references to provide sufficient evidence to support the Applicant's argument that the second multiplication circuit is not capable of receiving a bit of the first parameter and partial words of the second.

6. In response to the Applicant's argument that the applied reference does not teach pipelining stages, the Examiner disagrees. The sections cited by the Examiner, and again by the Applicant, disclose that all of the steps in are executing concurrently, thereby leading one of ordinary skill in the art to conclude that the process is being carried out in parallel, or pipelined. This is further supported by the disclosure of two multiplication circuits operating again in parallel. This is further supported by pages 45-60 of **Conception et Etude d'une Architecture**

**Numerique de Haute Performance pour le Calcul de la Fonction Exponentielle Modulaire**, by M. Alain Guyot, hereinafter Guyot, discloses that Montgomery's algorithm is a fast execution of modular multiplication. On pages 52-54, Guyot discloses using parallel processing to speed-up modular multiplication. Pipelining techniques for Montgomery products are well known, which is further supported by U.S. Patent Nos. 6,182,104 (column 1, lines 8-24), 6,061,706 (column 1, lines 7-13), 2002/0013799 (paragraph [0130]), 6,820,105 (column 19, lines 52-67), 6,668,267 (column 3, lines 25-64), 6,185,596 (column 4, lines 38-44), and 6,356,636 (column 1, lines 7-24).

7. In response to the Applicant's argument that Glaser fails to teach the field type being a prime field or a binary extension field, the Examiner respectfully disagrees. As Glaser discloses the use of prime fields at column 2, lines 38-46.

8. Therefore, it is held that Glaser discloses the field-type as claimed by the Applicant.

9. See further rejections that follow.

***Claim Rejections***

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-5, 12-15, and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,745,98 to Monier, hereinafter Monier, in view of U.S. Patent No. 6,397,241 to Glaser et al., hereinafter Glaser.

12. As per claim 1, Monier discloses a multiplication module, comprising:

a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B");

an output configured to deliver a Montgomery product of the first operand and the second operand (column 3, lines 38-45, column 7, lines 55-59, i.e. "a method for implementation of modular multiplication according to the Montgomery method").

13. Monier does not disclose a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation.

14. Glaser teaches a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

16. Regarding claim 2, Glaser discloses wherein the field select input is configurable to select a prime field representation or a binary extension field representation (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

17. With regards to claims 3 and 4, Monier teaches wherein the first operand is processed bit-wise and the second operand is processed word-wise (column 6, line 62 to column 7, line 46, column 9, lines 7-46).

18. Regarding claims 5, 9, 10, 13, 17, and 20, Monier discloses a dual-field adder that is configurable to execute addition without carry, based on a value supplied to the field select input (column 7, lines 19-23, column 10, lines 46-50).

19. As per claim 12, Monier discloses a dual-field adder, comprising:

a first input and a second input situated to receive respective operands (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B");

an addition module, configured to add values supplied to the first and second input according to a value supplied to the field-representation-select input (column 7, lines 19-23, column 10, lines 46-50).

20. Monier does not disclose a field-representation-select input.

21. Glaser teaches a field- representation-select input (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

23. With regards to claims 14 and 15, Monier discloses wherein the addition module includes an exclusive OR gate situated and configured to receive a bit of the first operand and a bit of the second operand (Figure 1 [blocks 30, 31]).

24. As per claim 19, Monier discloses a Montgomery multiplier configured to determine a Montgomery product of a first operand and a second operand, the multiplier comprising:

an output that delivers the Montgomery product (column 3, lines 38-45, column 7, lines 55-59).

25. Monier does not disclose a field-select input for selection of arithmetic operations corresponding to a prime field or a binary extension field.

26. Glaser teaches a field-select input for selection of arithmetic operations corresponding to a prime field or a binary extension field (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

27. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

28. With regards to claim 21, Monier discloses a scalable Montgomery multiplication module situated and configured to obtain a Montgomery product of the first operand and the second operand (column 3, lines 38-45, column 7, lines 55-59).

29. Claims 6, 7, and 16-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Monier.

30. As per claim 6, Monier discloses a cryptographic processor, comprising:

inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field (column 3, lines 38-45, column 5, lines 55-60, i.e. "multiplicand A and multiplier B"); and

a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including at least two processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter (Figure 1 [blocks 19, 20], column 3, lines 38-45, column 5, lines 27-37, column 7, lines 55-59).

31. Regarding claim 7, Monier discloses wherein at least one processing unit is configured to communicate intermediate values of partial words of the Montgomery product to a different processing unit (column 6, line 62 to column 7, line 46, column 9, lines 7-46).

32. As per claim 16, Monier discloses a method of determining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter, the method comprising:

representing the first cryptographic parameter as a series of bits (column 3, lines 38-45, column 5, lines 55-60);

representing the second cryptographic parameter as a series of words (column 3, lines 38-45, column 5, lines 55-60);

determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage (column 6, line 62 to column 7, line 46, column 9, lines 7-46);

determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage (column 6, line 62 to column 7, line 46, column 9, lines 7-46); and

combining the intermediate values to form the Montgomery product of the first cryptographic parameter and the second cryptographic parameter (column 3, lines 38-45, column 7, lines 55-59).

33. With regards to claim 18, Monier discloses a computer-readable medium containing instructions for executing the method of claim 17 (Figure 1 [block 35]).

34. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monier in view of Glaser OR Applicant's Admitted Prior Art, hereinafter AAPA.

35. Regarding claim 8, Monier does not teach a field-representation-select input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with *GF(p)* or *GF($2^m$)* arithmetic.

36. Glaser discloses a field-representation-select input in communication with the multiplication module for selection of an arithmetic operation in the multiplication module to be performed in accordance with *GF(p)* or *GF($2^m$)* arithmetic (column 2, lines 39-46, column 13, line 65 to column 14, line 32).

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation, since Glaser states at column 1, lines 30-35 that such a modification would achieve high performance, low cost, and low-power while being able to compute several different encryption algorithms.

38. AAPA discloses using GF($2^m$) and GF(p) on page 2 of the specification.

39. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement GF($2^m$), since AAPA discloses that there are efficient software implementations of such arithmetic, especially if an irreducible polynomial generating the finite field is chosen arbitrarily.

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement GF(p), since AAPA discloses that there are scalable Montgomery multiplier designs for this particular finite field.

41. Concerning claim 11, Monier teaches wherein the first and second cryptographic parameters are represented as *m* bits and *e* words of word length, wherein [(m + 1) / w] (column 4, lines 1-47).

***Conclusion***

42. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

43. The following patents are cited to further show the state of the art with respect to pipeline processing of Montgomery multipliers, such as:

United States Patent Application Publication No. 2005/0033790 to Hubert, which is cited to show pipelining in Montgomery multipliers.

44. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

45. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

46. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

47. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

48. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

CLL
Primary Examiner
AU 2131
12/9/05